AGENDA ITEM 4
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF NOVEMBER 30, 2007

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
Health Insurance Portability and Accountability Act (8/12/04)	Health Benefits Branch	1.1 CalPERS should develop comprehensive policies and procedures to maintain and demonstrate compliance with requirements of Health Insurance Portability and Accountability Act (HIPAA).	IN PROGRESS. HIPAA Administration is continuing coordination with Information Security to incorporate HIPAA security policies and procedures into the HIPAA portal. The division has submitted a corrective action plan with a target completion of December 31, 2007.
		2.1 CalPERS should ensure that its training program specifically identifies staff that require training, appropriate training to be provided, and ensure attendance at that training. Training documentation should demonstrate ongoing compliance with HIPAA requirements.	IN PROGRESS. HIPAA Administration is working with Information Security to develop and implement a computer-based training program which will provide the appropriate HIPAA training. Work is now scheduled to begin on the HIPAA computer-based training. The division has submitted a corrective action plan with a target completion of June 30, 2008.
		4.1 CalPERS should develop a continuous and formalized system to identify, update and document personal health information and staff access to the information.	IN PROGRESS. The existing policy and flowcharts are being reviewed and modified as appropriate. Once complete the policy and flow charts will be posted to the HIPAA portal. The division has submitted a corrective action plan with a target completion of December 31, 2007.
		6.1 CalPERS should develop a summary guide of the implementation and development process.	IN PROGRESS. The existing the ANSI 834 summary guide of compliance efforts located in the HIPAA Portal is being updated to accurately reflect implementation and development activity. The division has submitted a corrective action plan with a target completion of December 31, 2007.
HIPAA Security Compliance Review (10/20/06)		3.3 Health Benefits Branch, as data owner, has not established written polices and procedures that define roles and responsibilities for Electronic Protected Health Information access authorization. It should establish written policies and procedures for authorizing access to Electronic Protected Health Information owned by it.	IN PROGRESS. Written policies and procedures for authorizing access to Electronic Protected Health Information are being developed as part of the HIPAA e-compliance guide. Employer and Member Health Services has submitted a corrective action plan with a target completion of February 29, 2008.

AGENDA ITEM 4
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF NOVEMBER 30, 2007

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
HIPAA Security Compliance Review (10/20/06) *(continued)*	Health Benefits Branch	4.1 Health Benefits, as a data owner, has not established policies and procedures that clearly state how access to Electronic Protected Health Information should be granted. It should establish policies that will limit access to Electronic Protected Health Information to the minimum needed to carry out job functions.	IN PROGRESS. The HIPAA Privacy Officer is developing written policies and procedures for authorizing and limiting access to Electronic Protected Health Information as part of the HIPAA e-compliance guide. Employer and Member Health Services has submitted a corrective action plan with a target completion of February 29, 2008.
		9.1 CalPERS does not have an adequate process in place to identify all contractors requiring a business associate agreement. The HIPAA Privacy Officer should ensure that they develop and document a set of criteria for determining whether a contract is a business associate contract.	IN PROGRESS. The HIPAA Privacy Officer is developing a Business Associate Agreement decision tool for contract managers to use as a guide prior to execution of a contract. The decision tool will assist in determining if a firm meets the criteria to be considered a business associate. Employer and Member Health Services has submitted a corrective action plan with a target completion of February 29, 2008.
		9.2 The HIPAA Privacy Officer should work with the Information Security, Operations Support Services, and Health Benefits to develop a mechanism to identify all business associates when contracts are created.	IN PROGRESS. The HIPAA Privacy Officer is coordinating with Operations Support Services to develop a decision tool to ensure contracts are reviewed prior to execution and to determine if a business associate agreement is required. Employer and Member Health Services has submitted a corrective action plan with a target completion of February 29, 2008.
		9.3 The HIPAA Privacy Officer and Information Security should work together to identify all existing business associate contracts.	IN PROGRESS. The HIPAA Privacy Officer is coordinating with Office of Enterprise Compliance to establish a tool to identify existing contracts that require a business associate agreement. Employer and Member Health Services has submitted a corrective action plan with a target completion of February 29, 2008.

AGENDA ITEM 4
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF NOVEMBER 30, 2007

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
HIPAA Security Compliance Review (10/20/06) *(continued)*	Health Benefits Branch	11.2 Because CalPERS has not identified all information assets containing Electronic Protected Health Information, we were not able to locate a listing of workstations that can access Electronic Protected Health Information. Health Benefits should maintain an inventory of workstations having access to Electronic Protected Health Information.	IN PROGRESS. The HIPAA Privacy Officer will continue to update the HIPAA portal process flow charts and detail the workstation locations, users, etc. containing Electronic Protected Health Information. Employer and Member Health Services has submitted a corrective action plan with a target completion of March 31, 2008.
	Health Benefits/ Operations Support Services/ Information Security Office	7.2 Business continuity plan does not include procedures addressing the protection of Electronic Protected Health Information while operating in an emergency mode. Health Benefits, Operations Support and Information Security should review the plan to address the adequacy of protection.	IN PROGRESS. The Information Security Office is working with Health Benefits to review the Business Continuity Plan to ensure that adequate safeguards over protected health information are in place. This review is scheduled to complete in January 2008, at which time additional security requirements (if any) will be provided to the Operations Support Services. Operations Support services will meet new security requirements that do not require additional resources by March 2008. Any requirements needing additional resources and funding will be addressed through the regular budget cycle. A target completion date of March 31, 2008 has been set.
	Information Security Office	1.1 A thorough assessment has not been conducted of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all Electronic Protected Health Information. The Information Security Office should conduct this assessment.	IN PROGRESS. The Information Security Office states that it has received approval for three additional positions with which to develop and implement a risk assessment and management program. The risk analysis pilot program is projected to conclude in the first quarter of 2008, and it is expected to take two years for a full cycle of assessment. The Information Security Office plans corrective action completion by December 31, 2009.

AGENDA ITEM 4
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF NOVEMBER 30, 2007

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
HIPAA Security Compliance Review (10/20/06) *(continued)*	Information Security Office	1.2 CalPERS implements security measures to protect information assets housed at CalPERS to readily demonstrate HIPAA security compliance. Information Security Office should implement required security specifications and assess whether each addressable specification is a reasonable safeguard in the CalPERS environment based on risk analysis results.	IN PROGRESS. The Information Security Office states that this finding will be addressed as part of the IT infrastructure assessment scheduled for completion in February 2008 with the full assessment to be completed by September 2009.
		1.3 HIPAA security regulations require documentation of sanction policies. Sanctions taken against the violators may need to be documented for potential investigations. Information Security should consult with the Legal Office and revise the security practice, if necessary, to provide clear documentation guidelines.	IN PROGRESS. The Information Security Office has begun revising practices. It plans to finalize and publish updated security policies by June 2008.
		1.4 CalPERS' Event Logs Practice requires specific security events be logged at key servers. However, the practice does not specify which events must be logged at which system components, nor does it specify monitoring roles, responsibilities and frequency.	IN PROGRESS. The Information Security Office states that it plans to finalize and publish updated security policies by June 2008.
		3.1 CalPERS' Data Owners and Custodians Practice states that data owners are responsible for authorizing access to assets. However, it does not clearly state who should authorize logical access by technical support staff, and physical access to locations where Electronic Protected Health Information can be accessed.	IN PROGRESS. The Information Security Office states that it is preparing a new process by which data owners can give Information Technology Services senior management the authority to approve access for technical support staff. Information Technology Services will be required to establish access authorization processes that require two levels of approval. The new process should be in place by June 2008.

AGENDA ITEM 4
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF NOVEMBER 30, 2007

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
HIPAA Security Compliance Review (10/20/06) *(continued)*	Information Security Office	3.2 CalPERS' Data Owners and Custodians Practice is not clear on who should supervise employees and contractors working with Electronic Protected Health Information in areas that are outside the data owner's control. Information Security should establish or modify security practices to provide clearer guidelines.	IN PROGRESS. The Information Security Office states that it has purchased an appliance to assist data owners with monitoring responsibilities. It expects the appliance to be operational by June 2008.
		3.6 CalPERS has not performed a risk assessment to determine whether the current extent of employment screening process is sufficient for protecting Electronic Protected Health Information. Information Security, upon completion of risk analysis, should assess whether current screening is sufficient.	IN PROGRESS. Information Security Office states that this finding will be addressed at the conclusion of the IT infrastructure assessment scheduled for completion in February 2008.
		3.7 When employment of an Electronic Protected Health Information user ends divisions need to inform Security Administration in the stated timeframe. Information Security and Security Administration should provide training to enhance the security awareness among managers, authorized requestors, and system administrators.	COMPLETE. The Information Security Office has distributed email to managers, supervisors, PC contacts, and system administrators.
		3.9 CalPERS does not have a security practice that requires timely termination of physical access to locations where Electronic Protected Health Information can be accessed. Information Security should establish or revise current security practice to define the requirement.	IN PROGRESS. The Information Security Office has modified security practices that address the use and management of building access cards for the Lincoln Plaza Complex to ensure timely termination of physical access. It plans to finalize and publish updated security policies by June 2008.
		4.3 CalPERS' User Account Maintenance Practice requires timely modification of user access; however, it does not contain requirements regarding access establishment. Information Security should modify the practice to provide clearer guidelines.	IN PROGRESS. Information Security Office states that it has modified the Data Owner and Custodian Practice and published the Identity Authentication Practice. It plans to finalize security policy and Information Security Standards and Requirements by June 2008.

AGENDA ITEM 4
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF NOVEMBER 30, 2007

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
HIPAA Security Compliance Review (10/20/06) *(continued*	Information Security Office	5.1 CalPERS' Virus Practice requires anti-virus software to be installed on all CalPERS applicable computer server systems; however, it does not clearly define which servers are applicable. Information Security should revise the Practice to clarify which servers are required to have the software installed.	IN PROGRESS. The Information Security Office states that it has amended the practice to require all servers to have anti-virus software installed. In addition, it has submitted a mid-year budget request for funding to purchase a compliance monitoring tool. If the budget request is approved, the tool will be installed in the first half of 2008 and be fully functional by September 2008.
		5.2 CalPERS' Event Logs Practice requires logging of invalid user authentication attempts and unauthorized attempts to access resources. Information Security should incorporate current log-in monitoring practices into security risk analysis and risk mitigation strategy.	IN PROGRESS. The Information Security Office will evaluate the processes used to monitor invalid logon attempts as part of its IT infrastructure risk assessment scheduled to complete by February 2008. In addition, the Information Security Office has purchased a logging and monitoring tool. This tool will be operational by March 2008. Furthermore, it plans to publish updated security practice by March 2008 and updated policy and information security and requirements by June 2008.
		5.3 Information Technology Services uses systems to enforce password standards when feasible. Information Security should incorporate various administrators' current password practices into the security risk analysis and risk mitigation strategy.	IN PROGRESS. The Information Security Office has received approval for 3 positions to implement a Risk Assessment and Management Program. As part of this program, it will assess the IT infrastructure and the processes used to manage the infrastructure, including those used to manage administrators' passwords. Information Security Office has a target completion date of February 15, 2008 for this item.
		5.4 Deviations from the CalPERS Password Practice were not always supported with documented variances approved by Information Security. Information Security should ensure that system administrators implement procedures and comply with the Practice.	IN PROGRESS. The Information Security Office has identified a number of compliance monitoring tools. When these compliance monitoring tools are installed and implemented, it will be able to identify the systems that are non-compliant with password standards. The monitoring tools will be purchased by April 2008 and installed by September 2008.

AGENDA ITEM 4
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF NOVEMBER 30, 2007

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
HIPAA Security Compliance Review (10/20/06) *(continued)*	Information Security Office	6. CalPERS' Information Security Incidents Practice defines the events considered to be reportable incidents; however, current security practice and procedures do not adequately specify response efforts. Information Security should amend current security practices.	IN PROGRESS. The Information Security Office states that it will revise the security language in contract attachment by January 2008 to designate the CalPERS contract managers as the CalPERS contacts for security incident notifications. It has also increased security awareness training on security incident reporting. Its revised policy and Information Security Standards and Requirements will be published by June 2008.
		7.1 Information Technology Services does not regularly test the media that the Electronic Protected Health Information stored on to ensure that the information remains retrievable. Information Security should ensure that it establishes and implements procedures of testing.	COMPLETE. The Information Security Office has ensured that procedures for testing backup copies of the imaged documents have been established and implemented.
		7.3 Information security should ensure that senior management responsible for Electronic Protected Health Information determines the criticality of testing the applications retrieving Electronic Protected Health Information. The application retrieving Electronic Protected Health Information has not been included in previous tests.	IN PROGRESS. The Information Security Office stated that it has confirmed that FileNet is now included in the critical applications for testing and is tested during the regularly scheduled testing for business continuity, and it will provide supporting documentation for closing this issue in the near future.
		8.1 CalPERS has not conducted a thorough assessment of potential risks and vulnerabilities to Electronic Protected Health Information security. Information Security should establish security baselines upon completion of a risk analysis.	IN PROGRESS. The Information Security Office states that this finding will be addressed as part of the IT infrastructure assessment. Information Security Office set a target completion date of February 2008.
		8.2 Information Security should establish a process for periodic evaluation of administrative, physical, and technical safeguards in response to environmental or operational changes affecting the security of Electronic Protected Health Information.	IN PROGRESS. The Information Security Office states that this finding will be addressed as part of the IT infrastructure assessment and Health Benefits risk assessment scheduled for completion in February and April 2008.

AGENDA ITEM 4
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF NOVEMBER 30, 2007

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
HIPAA Security Compliance Review (10/20/06) *(continued)*	Information Security Office	8.4 CalPERS' Certification and Accreditation Practice requires that information applications and/or systems must undergo security certification and accreditation to certify that the information is protected. Information Security should ensure that this is performed periodically.	IN PROGRESS. The Information Security Office states that it is working with Information Technology Services to revise the certification and accreditation process. Information Security Office set a target completion date of March 2008.
		9.4 The Information Security Office should ensure that CalPERS develops appropriate security requirement provisions to be included in all existing and future business associate contracts.	IN PROGRESS. The Information Security Office is working with Health Benefits and Operations Support Services to complete the development of security requirement provisions for business associate contracts. Information Security Office plans to complete this item by December 31, 2007.
		10.1 CalPERS currently does not have a security practice that addresses granting facility access during an emergency. Information Security should establish security practices to outline physical security requirements.	IN PROGRESS. The Information Security Office has determined that the best way to ensure the integrity and confidentiality of information assets during an emergency is to have a single security policy that is applicable in all situations. This approach will be validated when implementing the Risk Assessment and Management Program. Information Security Office set a target completion date of April 2008.
		10.3 Currently, Information Security does not have information security practices addressing physical security. It should establish security practice(s) to specify facility security requirements based on the risk assessment.	IN PROGRESS. The Information Security Office states that it has revised the security policy and Information Security Standards and Requirements to define specific requirements for physical access to employee areas, data center, communication closets, and the operations recovery center. Desktop, laptop, and workstation location security are also addressed. Scheduled publication of the revised security policy and Information Security Standards and Requirements is June 2008.

AGENDA ITEM 4
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF NOVEMBER 30, 2007

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
HIPAA Security Compliance Review (10/20/06) *(continued)*	Information Security Office	10.5 CalPERS security practices do not require documentation of repairs and modifications to security related physical components of headquarter buildings. Information Security should establish a practice to require documentation.	IN PROGRESS. The Information Security Office states that it has revised the information security policy, which will be published in June 2008.
		11.1 CalPERS security practices do not specify proper functions to be performed on all different types of workstations, and physical attributes of the surroundings of a specific workstation. Information Security Office should establish these practices.	IN PROGRESS. The Information Security Office states that it has modified security practices to specify physical attributes of workstations based on its knowledge of how electronic protection health information can be accessed at CalPERS. It plans to conduct a security risk assessment with Health Benefits Branch between February and April of 2008 and with Member Services between May and July of 2008. During these risk assessments, the current approach will be validated. The security policy and Information Security Standards and Requirements will be published in June 2008.
		12. Because workstations are located in areas where physical access is more permissive than logical access, physical access alone does not restrict workstation access to only authorized users of Electronic Protected Health Information. Information Security should incorporate this as part of the risk analysis.	IN PROGRESS. The Information Security Office states that it has modified security practices to specify required physical and logical safeguards over workstations. It plans to conduct a security risk assessment with Health Benefits Branch between February and April of 2008 and with Member Services between May and July of 2008. During these risk assessments, current approach will be validated.
		13.2 Information Security practices do not specifically address media re-use. Media may include removable diskettes used by employees. Information Security Office should either amend the practices to specifically address media re-use or establish an additional practice.	IN PROGRESS. The Information Security Office has amended practices to specifically address media re-use. It will ensure that divisional policies and procedures are developed and implemented and will begin compliance monitoring by April 2008 contingent upon recruiting and training two new staff.

AGENDA ITEM 4
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF NOVEMBER 30, 2007

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
HIPAA Security Compliance Review (10/20/06) *(continued)*	Information Security Office	13.4 CalPERS' security practices do not specifically require the maintenance of records tracking the movements of hardware and electronic media internally. Information Security should determine if this is necessary and then establish or amend security practices as necessary.	IN PROGRESS. The Information Security Office states that this finding will be addressed as part of the IT infrastructure risk assessment scheduled for completion in February 2008 with implementation of any needed recommendations by April 2008.
		13.6 Current security practices and procedures do not require data backup to be created prior to moving equipment. Information security should address the need to require data to be backed up before movement of equipment.	IN PROGRESS. The Information Security Office states that it has included the requirement of making a complete backup prior to moving data to a different hardware platform in its Information Security Standards and Requirements. This approach will be validated during IT infrastructure risk assessment scheduled to complete in February 2008. If vulnerability is identified, the Information Security Office will work with Information Technology Services to define necessary processes. The Information Security Standards and Requirements will be published in June 2008.
		14.1 Technical support staff using shared accounts to access systems that maintain Electronic Protected Health Information do not always obtain an approved variance. Information Security should notify Security Administration upon identification of all systems containing Electronic Protected Health Information.	IN PROGRESS. The Information Security Office is working with Information Technology Services to replace existing shared IDs with unique ID's and to modify processes to no longer require use of shared ID's. The assessment should be completed by January 2008. Establishment of new processes and elimination of shared ID's should be completed by December 2008.
		14.3 CalPERS does not have a security practice that addresses access control during an emergency. Information Security should set forth security requirements that access should be restricted only to those persons that have been granted access rights during an emergency.	IN PROGRESS. The Information Security Office clarifies that all provisions and requirements defined in the security practices apply in all situations, including emergencies. The revised policy clearly stating this will be published no later than July 2008.

AGENDA ITEM 4
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF NOVEMBER 30, 2007

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
HIPAA Security Compliance Review (10/20/06) *(continued)*	Information Security Office	14.6 CalPERS does not require any data, including Electronic Protected Health Information, to be encrypted when sent across internal networks and while in storage. Information Security should address this need based on risk analysis results.	IN PROGRESS. The Information Security Office is conducting an IT infrastructure risk assessment. At conclusion, the ISOF will consider whether it is necessary to require encryption of data at-rest and in-motion on internal CalPERS-controlled networks. If yes, additional resources will be identified and funds will be requested through 2008-09 budget request process.
		15.1 CalPERS' Event Logs Practice does not require a retention period of 6 years or recording of functions performed. Information Security should modify the Event Logs Practice to require the recording and retention requirements.	IN PROGRESS. The Information Security Office is revising the Event Logs Practice. Information Technology Services has expressed concerns regarding the impact event logging would have on systems. The Information Security Office purchased an event logging appliance in May 2007. This tool is capable of collecting logs in such a manner that impact on system performance is expected to be minimal. The tool should be in production by June 2008 and the revised policy and Information Security Standards and Requirements should be published by July 2008.
		15.2 The Document Management System does not log who viewed imaged documents, or when and where the imaged documents are created, printed, exported, or viewed. The Event Logs Practice should be modified to provide clearer guidelines.	IN PROGRESS. The Information Security Office is revising the Event Logs Practice. Information Technology Services has expressed concerns regarding the impact event logging would have on systems. The Information Security Office purchased an event logging appliance in May 2007. This tool is capable of collecting and printing logs in such a manner that impact on system performance is expected to be minimal. The tool should be in production by June 2008 and the revised policy and Information Security Standards and Requirements should be published by July 2008.

AGENDA ITEM 4
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF NOVEMBER 30, 2007

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
HIPAA Security Compliance Review (10/20/06) *(continued)*	Information Security Office	16. A thorough risk analysis of the technical environment in which all Electronic Protected Health Information resides has not been conducted. Upon completion of risk analysis, Information Security should document the controls utilized to corroborate that Electronic Protected Health Information has not been altered or destroyed in an unauthorized manner.	IN PROGRESS. The Information Security Office is conducting the IT infrastructure risk assessment scheduled for completion in February 2008. At conclusion, the Information Security Office will document existing security controls and deficiencies. Additional resources may be required to implement remediation.
		18. Because CalPERS has not identified all the locations where Electronic Protected Health Information resides, we cannot determine whether current security measures are adequate. Information Security should determine whether additional controls are needed to ensure that Electronic Protected Health Information is properly protected during transmission.	IN PROGRESS. The Information Security Office states that this finding will be addressed as part of the IT infrastructure risk assessment scheduled for completion in February 2008 with detailed data mapping to be completed by August 2008. Should additional encryption technology be required, it would be requested as part of fiscal year 2008-09 and 2009-10 formal budget request process.
	Information Security Office/ Health Benefits	17. Once authorized users log into the network via their desktop computer they are not authenticated again by Document Management System prior to accessing Electronic Protected Health Information. Information Security and Health Benefits should work with Technology Services Support to determine whether users should be authenticated by Document Management System prior to accessing Electronic Protected Health Information.	IN PROGRESS. The HIPAA Privacy Officer will continue to work with Information Security to determine whether the Document Management System should require user authentication prior to accessing Electronic Protected Health Information. Health Benefits has submitted a corrective action plan with a target completion date of March 31, 2008. The Information Security Office indicates that it requested two positions that will be used to augment compliance monitoring activities, and plans corrective action with a target completion date of April 2008.
	Information Technology Services	3.8 Some access terminations were not supported with appropriate request forms. Information Technology Services should improve documentation for termination of logical access to Electronic Protected Health Information so as to demonstrate compliance.	COMPLETE. Information Technology Services Security Administration has improved documentation of the termination of logical access to Electronic Protected Health Information within Document Management System.

AGENDA ITEM 4
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF NOVEMBER 30, 2007

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
HIPAA Security Compliance Review (10/20/06) *(continued)*	Information Technology Services	13.5 Information Technology Services does not maintain an inventory policy for devices and electronic media. Upon Information Security's completion of security practice regarding tracking of hardware and electronic media, they should amend their policy manual to ensure compliance.	IN PROGRESS. Information Technology Services Security Administration states that once the Information Security Office completes their risk assessment and security practices regarding tracking of hardware and electronic media, Information Technology Services will amend their policy manual to ensure compliance. A corrective action plan was submitted; the target completion date is pending completion of tasks by the Information Security Office.
	Operations Support Services	3.5 Operations Support Services does not have written policies for authorizing physical access to CalPERS buildings. It should consult with Information Security regarding physical access controls.	COMPLETE. Operations Support Services has implemented policies and procedures for authorizing physical access to CalPERS' Lincoln Plaza Complex.
		4.2 Operations Support Services does not have written polices and procedures that specify how physical access can be granted to employees and contractors. It should establish policies and procedures and consult with Health Benefits regarding Electronic Protected Health Information protection requirements.	COMPLETE. Operations Support Services has implemented policies and procedures for authorizing physical access to CalPERS' Lincoln Plaza Complex.
		4.5 Operations Support Services utilizes a card access request form to document users' rights to various business areas. However, the form does not have written instructions on how to use it. It should improve and retain documentation to support the level of access granted to staff.	COMPLETE. Operations Support Services has established building access policies and procedures, revised access card request forms, created instructions for completing and processing the access card request forms, and provided training to divisional representatives to ensure users' rights of building access are properly established and modified when necessary.
		10.2 Operations System Support has not established written procedures for allowing access to the Emergency Operation Center in the event of an emergency. It should establish written procedures for allowing facility access.	COMPLETE. Operations Support Services has established written procedures for allowing access to the Emergency Operation Center in the event of an emergency.

AGENDA ITEM 4
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF NOVEMBER 30, 2007

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
HIPAA Security Compliance Review (10/20/06) *(continued)*	Operations Support Services	10.4 Policies and procedure should be implemented to control and validate physical access to its electronic information systems. Operations Support Services has no written access validation procedures.	COMPLETE. Operations Support Services has established written procedures for access validation procedures for the Lincoln Plaza Complex, including the data center, as well as the Emergency Operations Center.
	Security Administration	4.4 Security Administration uses software that is not configured to require data owner approval. They should modify its access management process and procedures to ensure compliance with CalPERS security practices and proper documentation of access authorization, review, and modification.	COMPLETE. Information Technology Services Security Administration has improved access management processes and procedures to ensure compliance with CalPERS security practices and proper documentation of access authorization, review, and modification of logical access to Electronic Protected Health Information within the Document Management System.
		8.3 Security Administration should ensure timely implementation of technical safeguards once the security baselines are established and updated.	IN PROGRESS. Information Technology Services, Security Administration, is developing the Security Certification and Accreditation Process. This process is expected to be completed by June 30, 2008. Once all systems containing HIPAA data are identified by the Information Security Office, Security Administration will schedule those systems for the certification process. A corrective action plan was submitted. The target completion date is pending Information Security Office's identification of all systems containing HIPAA data.

AGENDA ITEM 4
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF NOVEMBER 30, 2007

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
HIPAA Security Compliance Review (10/20/06) *(continued)*	Security Administration	14.2 Technical support staff using shared accounts to access systems that maintain Electronic Protected Health Information do not always obtain an approved variance. Security Administration should ensure that all users have a unique identifier. An approved variance should be obtained and documented for all shared IDs.	IN PROGRESS. Information Technology Services Security Administration is identifying owners and locations of shared accounts. Security Administration will then work with the account owners to remove the shared accounts. As other systems containing electronic protected health information are identified by the Information Security Office during its IT infrastructure risk assessment, Security Administration will follow up to resolve the issue. To eliminate future problems with shared accounts, Security Administration has changed procedures to reject all requests of a shared account without an approval from the Information Security Office.